The Symmetry Group of Gaussian States in $L^2(\mathbb{R}^n)$

K. R. Parthasarathy

Abstract This is a continuation of the expository article [4] with some new remarks. Let S_n denote the set of all Gaussian states in the complex Hilbert space $L^2(\mathbb{R}^n)$, K_n the convex set of all momentum and position covariance matrices of order $2n$ in Gaussian states and let $\mathscr{G}_n$ be the group of all unitary operators in $L^2(\mathbb{R}^n)$ conjugations by which leave S_n invariant. Here we prove the following results. K_n is a closed convex set for which a matrix S is an extreme point if and only if $S = \frac{1}{2}L^T L$ for some L in the symplectic group $Sp(2n,\mathbb{R})$. Every element in K_n is of the form $\frac{1}{2}(L^T L + M^T M)$ for some L, M in $Sp(2n,\mathbb{R})$. Every Gaussian state in $L^2(\mathbb{R}^n)$ can be purified to a Gaussian state in $L^2(\mathbb{R}^{2n})$. Any element U in the group $\mathscr{G}_n$ is of the form $U = \lambda W(\boldsymbol{\alpha})\Gamma(L)$ where λ is a complex scalar of modulus unity, $\boldsymbol{\alpha} \in \mathbb{C}^n$, $L \in Sp(2n,\mathbb{R})$, $W(\boldsymbol{\alpha})$ is the Weyl operator corresponding to $\boldsymbol{\alpha}$ and $\Gamma(L)$ is a unitary operator which implements the Bogolioubov automorphism of the Lie algebra generated by the canonical momentum and position observables induced by the symplectic linear transformation L.

Acknowledgements The author thanks Professor R. Simon and Professor M. Krishna for several fruitful conversations on this subject during July-August 2010 and the Institute of Mathematical Sciences, Chennai for their warm hospitality.

2000 Mathematics subject classification 81S25; 60B15, 42A82, 81R30.

Key words: Gaussian state, momentum and position observables, Weyl operators, symplectic group, Bogolioubov automorphism

---

K. R. Parthasarathy
Indian Statistical Institute, 7, S. J. S. Sansanwal Marg, New Delhi - 110016, India, e-mail: `krp@isid.ac.in`

1 Introduction

In [4] we defined a quantum Gaussian state in $L^2(\mathbb{R}^n)$ as a state in which every real linear combination of the canonical momentum and position observables $p_1, p_2, \ldots, p_n;\ q_1, q_2, \ldots, q_n$ has a normal distribution on the real line. Such a state is uniquely determined by the expectation values of $p_1, p_2, \ldots, p_n;\ q_1, q_2, \ldots, q_n$ and their covariance matrix of order $2n$. A real positive definite matrix S of order $2n$ is the covariance matrix of the observables $p_1, p_2, \ldots, p_n;\ q_1, q_2, \ldots, q_n$ if and only if the matrix inequality

$$2S - i\,J \geq 0 \tag{1.1}$$

holds where

$$J = \begin{bmatrix} 0 & -I \\ I & 0 \end{bmatrix}, \tag{1.2}$$

the right hand side being expressed in block notation with 0 and I being of order $n \times n$. We denote by K_n the set of all possible covariance matrices of the momentum and position observables in Gaussian states so that

$$K_n = \left\{ S | S \text{ is a real symmetric matrix of order } 2n \text{ and } 2S - iJ \geq 0 \right\}. \tag{1.3}$$

Clearly, K_n is a closed convex set. Here we shall show that S is an extreme point of K_n if and only if $S = \frac{1}{2} L^T L$ for some matrix L in the real symplectic matrix group

$$Sp(2n, \mathbb{R}) = \left\{ L | L^T J L = J \right\} \tag{1.4}$$

with the superfix T indicating transpose. Furthermore, it turns out that every element S in K_n can be expressed as

$$S = \frac{1}{2}(L^T L + M^T M)$$

for some $L, M \in Sp(2n, \mathbb{R})$. This, in turn implies that any Gaussian state in $L^2(\mathbb{R}^n)$ can be purified to a pure Gaussian state in $L^2(\mathbb{R}^{2n})$.

Let $\boldsymbol{\alpha} \in (\alpha_1, \alpha_2, \ldots, \alpha_n)^T \in \mathbb{C}^n$, $L = ((\ell_{ij})) \in Sp(2n, \mathbb{R})$ and let $\alpha_j = x_j + iy_j$ with $x_j, y_j \in \mathbb{R}$. Define a new set of momentum and position observables $p_1', p_2', \ldots, p_n';$ $q_1', q_2', \ldots, q_n'$ by

$$\begin{aligned} p_i' &= \sum_{j=1}^{n} \left\{ \ell_{ij}(p_j - x_j) + \ell_{in+j}(q_j - y_j) \right\}, \\ q_i' &= \sum_{j=1}^{n} \left\{ \ell_{n+i\,j}(p_j - x_j) + \ell_{n+i\,n+j}(q_j - y_j) \right\}, \end{aligned}$$

for $1 \leq i \leq n$. Here one takes linear combinations and their respective closures to obtain p_i', q_i' as selfadjoint operator observables. Then $p_i', p_2', \ldots, p_n';\ q_i', q_2', \ldots, q_n'$

obey the canonical commutation relations and thanks to the Stone-von Neumann uniqueness theorem there exists a unitary operator $\Gamma(\boldsymbol{\alpha}, L)$ satisfying

$$p_i' = \Gamma(\boldsymbol{\alpha}, L)\ p_i\ \Gamma(\boldsymbol{\alpha}, L)^\dagger,$$
$$q_i' = \Gamma(\boldsymbol{\alpha}, L)\ q_i\ \Gamma(\boldsymbol{\alpha}, L)^\dagger$$

for all $1 \leq i \leq n$. Furthermore, such a $\Gamma(\boldsymbol{\alpha}, L)$ is unique upto a scalar multiple of modulus unity. The correspondence $(\boldsymbol{\alpha}, L) \to \Gamma(\boldsymbol{\alpha}, L)$ is a projective unitary and irreducible representation of the semidirect product group $\mathbb{C}^n \circledS Sp(2n, \mathbb{R})$. Here any element L of $Sp(2n, \mathbb{R})$ acts on $\mathbb{C}^n$ real-linearly preserving the imaginary part of the scalar product. The operator $\Gamma(\boldsymbol{\alpha}, L)$ can be expressed as the product of $W(\boldsymbol{\alpha}) = \Gamma(\boldsymbol{\alpha}, I)$ and $\Gamma(L) = \Gamma(\mathbf{0}, L)$. Conjugations by $W(\boldsymbol{\alpha})$ implement translations of p_j, q_j by scalars whereas conjugations by $\Gamma(L)$ implement symplectic linear transformations by elements of $Sp(2n, \mathbb{R})$, which are the so-called Bogolioubov automorphisms of canonical commutation relations. In the last section we show that every unitary operator U in $L^2(\mathbb{R}^n)$, with the property that $U\rho U^\dagger$ is a Gaussian state whenever ρ is a Gaussian state, has the form $U = \lambda W(\boldsymbol{\alpha})\Gamma(L)$ for some scalar λ of modulus unity, a vector $\boldsymbol{\alpha}$ in $\mathbb{C}^n$ and a matrix L in the group $Sp(2n, \mathbb{R})$.

The following two natural problems that arise in the context of our note seem to be open. What is the most general unitary operator U in $L^2(\mathbb{R}^n)$ with the property that whenever $|\psi\rangle$ is a pure Gaussian state so is $U|\psi\rangle$? Secondly, what is the most general trace-preserving and completely positive linear map Λ on the ideal of trace-class operators on $L^2(\mathbb{R}^n)$ with the property that $\Lambda(\rho)$ is a Gaussian state whenever ρ is a Gaussian state?

2 Exponential vectors, Weyl operators, second quantization and the quantum Fourier transform

For any $\boldsymbol{z} = (z_1, z_2, \ldots, z_n)^T$ in $\mathbb{C}^n$ define the associated *exponential vector* $e(\boldsymbol{z})$ in $L^2(\mathbb{R}^n)$ by

$$e(\boldsymbol{z})(\boldsymbol{x}) = (2\pi)^{-n/4} \exp \sum_{j=1}^{n} (\boldsymbol{z}_j \boldsymbol{x}_j - \frac{1}{2}\boldsymbol{z}_j^2 - \frac{1}{4}\boldsymbol{x}_j^2). \tag{2.1}$$

Writing scalar products in the Dirac notation we have

$$\begin{aligned} \langle e(\boldsymbol{z}) | e(\boldsymbol{z}') \rangle &= \exp \langle \boldsymbol{z} | \boldsymbol{z}' \rangle \\ &= \exp \sum_{j=1}^{n} \bar{z}_j z_j'. \end{aligned} \tag{2.2}$$

The exponential vectors constitute a linearly independent and total set in the Hilbert space $L^2(\mathbb{R}^n)$. If U is a unitary matrix of order n then there exists a unique unitary $\Gamma(U)$ in $L^2(\mathbb{R}^n)$ satisfying

$$\Gamma(U)|e(\boldsymbol{z})\rangle = |e(U\boldsymbol{z})\rangle \quad \forall\, \boldsymbol{z} \in \mathbb{C}^n. \tag{2.3}$$

The operator $\Gamma(U)$ is called the *second quantization* of U. For any two unitary matrices U,V in the unitary group $\mathscr{U}(n)$ one has

$$\Gamma(U)\Gamma(V) = \Gamma(UV).$$

The correspondence $U \to \Gamma(U)$ is a strongly continuous unitary representation of the group $\mathscr{U}(n)$ of all unitary matrices of order n.

For any $\boldsymbol{\alpha} \in \mathbb{C}^n$ there is a unique unitary operator $W(\boldsymbol{\alpha})$ in $L^2(\mathbb{R}^n)$ satisfying

$$W(\boldsymbol{\alpha})\, |e(\boldsymbol{z})\rangle = e^{-\frac{1}{2}\|\boldsymbol{\alpha}\|^2 - \langle \boldsymbol{\alpha}|\boldsymbol{z}\rangle}\, |e(\boldsymbol{z}+\boldsymbol{\alpha})\rangle \quad \forall \quad \boldsymbol{z} \in \mathbb{C}^n. \tag{2.4}$$

For any $\boldsymbol{\alpha}, \boldsymbol{\beta}$ in $\mathbb{C}^n$ one has

$$W(\boldsymbol{\alpha})\, W(\boldsymbol{\beta}) = e^{-i\,\mathrm{Im}\langle \boldsymbol{\alpha}|\boldsymbol{\beta}\rangle}\, W(\boldsymbol{\alpha}+\boldsymbol{\beta}). \tag{2.5}$$

The correspondence $\boldsymbol{\alpha} \to W(\boldsymbol{\alpha})$ is a projective unitary and irreducible representation of the additive group $\mathbb{C}^n$. The operator $W(\boldsymbol{\alpha})$ is called the *Weyl operator* associated with $\boldsymbol{\alpha}$. As a consequence of (2.5) it follows that the map $t \to W(t\boldsymbol{\alpha})$, $t \in \mathbb{R}$ is a strongly continuous one parameter unitary group admitting a selfadjoint Stone generator $p(\boldsymbol{\alpha})$ such that

$$W(t\boldsymbol{\alpha}) = e^{-itp(\boldsymbol{\alpha})} \quad \forall \quad \boldsymbol{\alpha} \in \mathbb{C}^n. \tag{2.6}$$

Writing $\boldsymbol{e}_j = (0,0,\ldots,0,1,0,\ldots,0)^T$ with 1 in the j-th position,

$$p_j = 2^{-\frac{1}{2}}\, p(\boldsymbol{e}_j), \quad q_j = -2^{-\frac{1}{2}} p(i\boldsymbol{e}_j) \tag{2.7}$$

$$a_j = \frac{q_j + ip_j}{\sqrt{2}}, \quad a_j^\dagger = \frac{q_j - ip_j}{\sqrt{2}} \tag{2.8}$$

one obtains a realization of the momentum and position observables $p_j, q_j, 1 \le i \le n$ obeying the canonical commutation relations (CCR)

$$[p_i, p_j] = 0, \quad [q_i, q_j] = 0, \quad [q_r, p_s] = i\delta_{rs}$$

and the adjoint pairs a_j, $a_j^\dagger$ of annihilation and creation operators satisfying

$$[a_i, a_j] = 0, \quad [a_i, a_j^\dagger] = \delta_{ij}$$

in appropriate domains. If we write

$$p_j^s = 2^{-\frac{1}{2}} p_j, \quad q_j^s = 2^{\frac{1}{2}} q_j$$

one obtains the canonical Schrödinger pairs of momentum and position observables in the form

$$\left(p_j^s\psi\right)(\boldsymbol{x}) = \frac{1}{i}\,\frac{\partial\psi}{\partial x_j}(\boldsymbol{x}),\left(q_j^s\psi\right)(\boldsymbol{x}) = x_j\ \psi(\boldsymbol{x})$$

in appropriate domains. We refer to [5] for more details.

We now introduce the sympletic group $Sp(2n,\mathbb{R})$ of real matrices of order $2n$ satisfying (1.4). Any element of this group is called a symplectic matrix. As described in [1], [4], for any symplectic matrix L there exists a unitary operator $\Gamma(L)$ satisfying

$$\Gamma(L)\,W(\boldsymbol{\alpha})\,\Gamma(L)^{\dagger} = W(\tilde{L}\boldsymbol{\alpha}) \quad \forall \quad \boldsymbol{\alpha}\in\mathbb{C}^n \tag{2.9}$$

where

$$\begin{bmatrix}\mathrm{Re}\ \tilde{L}\boldsymbol{\alpha}\\ \mathrm{Im}\ \tilde{L}\boldsymbol{\alpha}\end{bmatrix} = L\ \begin{bmatrix}\mathrm{Re}\ \boldsymbol{\alpha}\\ \mathrm{Im}\ \boldsymbol{\alpha}\end{bmatrix}. \tag{2.10}$$

Whenever the symplectic matrix L is also a real orthogonal matrix then $\tilde{L}$ is a unitary matrix and $\Gamma(L)$ coincides with the second quantization $\Gamma(\tilde{L})$ of $\tilde{L}$. Conversely, if U is a unitary matrix of order n, L_U is the matrix satisfying

$$L_U\begin{bmatrix}\boldsymbol{x}\\ \boldsymbol{y}\end{bmatrix} = \begin{bmatrix}\mathrm{Re}\ U(\boldsymbol{x}+i\boldsymbol{y})\\ \mathrm{Im}\ U(\boldsymbol{x}+i\boldsymbol{y})\end{bmatrix}$$

then L_U is a symplectic and real orthogonal matrix of order $2n$ and $\Gamma(L_U) = \Gamma(U)$. Equations (2.9) and (2.6) imply that $\Gamma(L)$ implements the Bogolioubov automorphism determined by the symplectic matrix L through conjugation.

For any state ρ in $L^2(\mathbb{R}^n)$ its *quantum Fourier transform* $\hat{\rho}$ is defined to be the complex-valued function on $\mathbb{C}^n$ given by

$$\hat{\rho}(\boldsymbol{\alpha}) = \mathrm{Tr}\,\rho\,W(\boldsymbol{\alpha}), \quad \boldsymbol{\alpha}\in\mathbb{C}^n. \tag{2.11}$$

In [4] we have described a necessary and sufficient condition for a complex-valued function f on $\mathbb{C}^n$ to be the quantum Fourier transform of a state in $L^2(\mathbb{R}^n)$. Here we shall briefly describe an inversion formula for reconstructing ρ from $\hat{\rho}$. To this end we first observe that (2.11) is well defined whenever ρ is any trace-class operator in $L^2(\mathbb{R})$. Denote by $\mathscr{F}_1$ and $\mathscr{F}_2$ respectively the ideals of trace-class and Hilbert-Schmidt operators in $L^2(\mathbb{R}^n)$. Then $\mathscr{F}_1\subset\mathscr{F}_2$ and $\mathscr{F}_2$ is a Hilbert space with the inner product $\langle A|B\rangle = \mathrm{Tr}A^{\dagger}B$. There is a natural isomorphism between $\mathscr{F}_2$ and $L^2(\mathbb{R}^n)\otimes L^2(\mathbb{R}^n)$, which can, in turn, be identified with the Hilbert space of square integrable functions of two variables $\boldsymbol{x},\boldsymbol{y}$ in $\mathbb{R}^n$. We denote this isomorphism by $\mathscr{I}$ so that $\mathscr{I}(A)(\boldsymbol{x},\boldsymbol{y})$ is a square integrable function of $(\boldsymbol{x},\boldsymbol{y})$ for any $A\in\mathscr{F}_2$ and

$$\mathscr{I}(|e(\boldsymbol{u})\rangle\langle e(\overline{\boldsymbol{v}})|)(\boldsymbol{x},\boldsymbol{y}) = e(\boldsymbol{u})(\boldsymbol{x})e(\boldsymbol{v})(\boldsymbol{y}) \tag{2.12}$$

for all $\boldsymbol{u}$, $\boldsymbol{v}\in\mathbb{C}^n$, $\overline{\boldsymbol{v}}$ denoting $(\overline{v}_1,\overline{v}_2,\ldots,\overline{v}_n)$. From (2.4) and (2.11) we have

$$\begin{aligned}(|e(\boldsymbol{u})\rangle\langle e(\overline{\boldsymbol{v}})|)^{\wedge}(\boldsymbol{\alpha}) &= \langle e(\overline{\boldsymbol{v}})\,|W(\boldsymbol{\alpha})|\,e(\boldsymbol{u})\rangle\\ &= \exp\left\{-\frac{1}{2}\|\boldsymbol{\alpha}\|^2 - \langle\boldsymbol{\alpha}|\boldsymbol{u}\rangle + \langle\overline{\boldsymbol{v}}|\boldsymbol{\alpha}\rangle + \langle\boldsymbol{v}|\boldsymbol{u}\rangle\right\}.\end{aligned}$$

Substituting $\boldsymbol{\alpha} = \boldsymbol{x} + i\boldsymbol{y}$ and using (2.1), the equation above, after some algebra, can be expressed as

$$(|e(\boldsymbol{u})\rangle\langle e(\overline{\boldsymbol{v}})|)^{\wedge}(\boldsymbol{x}+i\boldsymbol{y}) = (2\pi)^{n/2} e(\boldsymbol{u}')(\sqrt{2}\boldsymbol{x}) e(\boldsymbol{v}')(\sqrt{2}\boldsymbol{y}) \tag{2.13}$$

where

$$\begin{aligned} \begin{bmatrix} \boldsymbol{u}' \\ \boldsymbol{v}' \end{bmatrix} &= U \begin{bmatrix} \boldsymbol{u} \\ \boldsymbol{v} \end{bmatrix}, \\ U &= 2^{-1/2} \begin{bmatrix} -I & I \\ iI & iI \end{bmatrix}. \end{aligned} \tag{2.14}$$

Let $D_\theta, \theta > 0$ denote the unitary dilation operator in $L^2(\mathbb{R}^n) \otimes L^2(\mathbb{R}^n)$ defined by

$$(D_\theta f)(\boldsymbol{x}, \boldsymbol{y}) = \theta^n f(\theta \boldsymbol{x}, \theta \boldsymbol{y}). \tag{2.15}$$

Then (2.13) can be expressed as

$$(|e(\boldsymbol{u})\rangle\langle e(\overline{\boldsymbol{v}}|)^{\wedge}(\boldsymbol{x}+i\boldsymbol{y}) = \pi^{n/2} \left\{ D_{\sqrt{2}} \Gamma(U) e(\boldsymbol{u} \otimes \boldsymbol{v}) \right\} (\boldsymbol{x}, \boldsymbol{y})$$

where $\Gamma(U)$ is the second quantization operator in $L^2(\mathbb{R}^{2n})$ associated with the unitary matrix U in (2.14) of order $2n$. Since exponential vectors are total and $D_{\sqrt{2}}$ and $\Gamma(U)$ are unitary we can express the quantum Fourier transform $\rho \to \hat{\rho}(\boldsymbol{x}+i\boldsymbol{y})$ as

$$\hat{\rho} = \pi^{n/2} D_{\sqrt{2}}\, \Gamma(U)\, \mathscr{I}(\rho). \tag{2.16}$$

In particular, $\hat{\rho}(\boldsymbol{x}+i\boldsymbol{y})$ is a square integrable function of $(\boldsymbol{x}, \boldsymbol{y}) \in \mathbb{R}^n \times \mathbb{R}^n$ and

$$\rho = \pi^{-n/2}\, \mathscr{I}^{-1}\, \Gamma(U^\dagger)\, D_{2^{-1/2}}\, \hat{\rho} \tag{2.17}$$

is the required inversion formula for the quantum Fourier transform. It is a curious but an elementary fact that the eigenvalues of U in (2.14) are all 12^{th} roots of unity and hence the unitary operators $\Gamma(U)$ and $\Gamma(U^\dagger)$ appearing in (2.16) and (2.17) have their 12-th powers equal to identity. This may be viewed as a quantum analogue of the classical fact that the 4-th power of the unitary Fourier transform in $L^2(\mathbb{R}^n)$ is equal to identity.

3 Gaussian states and their covariance matrices

We begin by choosing and fixing the canonical momentum and position observables $p_1, p_2, \ldots, p_n; q_1, q_2, \ldots, q_n$ as in equation (2.7) in terms of the Weyl operators. They obey the CCR. The closure of any real linear combination of the form $\sum_{j=1}^{n} (x_j p_j - y_j q_j)$ is selfadjoint and we denote the resulting observable by the same symbol. As

in [4], for $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_n)^T$, $\alpha_j = x_j + iy_j$ with x_j, $y_j \in \mathbb{R}$, the Weyl operator $W(\boldsymbol{\alpha})$ defined in Section 2 can be expressed as

$$W(\boldsymbol{\alpha}) = e^{-i\sqrt{2}\sum\limits_{j=1}^{n}(x_j p_j - y_j q_j)}. \tag{3.1}$$

Sometimes it is useful to express $W(\boldsymbol{\alpha})$ in terms of the annihilation and creation operators defined by (2.8):

$$W(\boldsymbol{\alpha}) = e^{\sum\limits_{j=1}^{n}(\alpha_j a_j^\dagger - \bar{\alpha}_j a_j)} \tag{3.2}$$

where the linear combination in the exponent is the closed version. A state ρ in $L^2(\mathbb{R})$ is said to be *Gaussian* if every observable of the form $\sum\limits_{j=1}^{n}(x_j p_j - y_j q_j)$ has a normal distribution on the real line in the state ρ for $x_j, y_j \in \mathbb{R}$. From [4] we have the following theorem.

Theorem 1. *A state ρ in $L^2(\mathbb{R}^n)$ is Gaussian if and only if its quantum Fourier transform $\hat{\rho}$ is given by*

$$\begin{aligned}\hat{\rho}(\boldsymbol{\alpha}) &= \operatorname{Tr} \rho\, W(\boldsymbol{\alpha}) \\ &= \exp\left\{-i\sqrt{2}\left(\boldsymbol{\ell}^T \boldsymbol{x} - \boldsymbol{m}^T \boldsymbol{y}\right) - \left(\boldsymbol{x}^T, \boldsymbol{y}^T\right) S \begin{pmatrix} \boldsymbol{x} \\ \boldsymbol{y} \end{pmatrix}\right\}\end{aligned} \tag{3.3}$$

for every $\boldsymbol{\alpha} = \boldsymbol{x} + i\boldsymbol{y}$, $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{R}^n$ where $\boldsymbol{\ell}$, $\boldsymbol{m}$ are vectors in $\mathbb{R}^n$ and S is a real positive definite matrix of order $2n$ satisfying the matrix inequality $2S - iJ \geq 0$, with J as in (1.2).

Proof. We refer to the proof of Theorem 3.1 in [4]. $\square$

We remark that $\boldsymbol{\ell}$, $\boldsymbol{m}$ and S in (3.3) are defined by the equations

$$\boldsymbol{\ell}^T \boldsymbol{x} - \boldsymbol{m}^T \boldsymbol{y} = \operatorname{Tr} \rho \sum_{j=1}^{n}(x_j p_j - y_j q_j)$$

$$(\boldsymbol{x}^T, \boldsymbol{y}^T) S \begin{pmatrix} \boldsymbol{x} \\ \boldsymbol{y} \end{pmatrix} = \operatorname{Tr} \rho\, X^2 - (\operatorname{Tr} \rho X)^2, X = \sum_{j=1}^{n}(x_j p_j - y_j q_j).$$

It is clear that ℓ_j is the expectation value of p_j, m_j is the expectation value of q_j and S is the covariance matrix of $p_1, p_2, \ldots, p_n$; $-q_1, -q_2, \ldots, -q_n$ in the state ρ defined by (3.3). By a slight abuse of language we call S the covariance matrix of the Gaussian state ρ. All such Gaussian covariance matrices constitute the convex set K_n defined already in (1.3). We shall now investigate some properties of this convex set.

Proposition 1 (Williamson's normal form [1]). *Let A be any real strictly positive definite matrix of order $2n$. Then there exists a unique diagonal matrix D of order n*

with diagonal entries $d_1 \geq d_2 \geq \cdots \geq d_n > 0$ *and a symplectic matrix* M *in* $Sp(2n,\mathbb{R})$ *such that*

$$A = M^T \begin{bmatrix} D & 0 \\ 0 & D \end{bmatrix} M. \tag{3.4}$$

Proof. Define

$$B = A^{1/2}\, J A^{1/2}$$

where J is given by (1.2). Then B is a real skew symmetric matrix of full rank. Hence its eigenvalues, inclusive of multiplicity, can be arranged as $\pm id_1, \pm id_2, \ldots, \pm id_n$ where $d_1 \geq d_2 \geq \cdots \geq d_n > 0$. Define $D = \mathrm{diag}(d_1, d_2, \ldots, d_n)$, i.e., the diagonal matrix with d_i as the ii-th entry for $1 \leq i \leq n$. Then there exists a real orthogonal matrix Γ of order $2n$ such that

$$\Gamma^T B \Gamma = \begin{bmatrix} 0 & -D \\ D & 0 \end{bmatrix}.$$

Define

$$L = A^{1/2}\,\Gamma \begin{bmatrix} D^{-1/2} & 0 \\ 0 & D^{-1/2} \end{bmatrix}.$$

Then $L^T J L = J$ and

$$LAL^T = \begin{bmatrix} D & 0 \\ 0 & D \end{bmatrix}.$$

Putting $M = (L^{-1})^T$ we obtain (3.4).

To prove the uniqueness of D, suppose $D' = \mathrm{diag}(d'_1, d'_2, \ldots, d'_n)$ with $d'_1 \geq d'_2 \geq \cdots \geq d'_n > 0$ and M' is another symplectic matrix of order $2n$ such that

$$A = M^T \begin{bmatrix} D & 0 \\ 0 & D \end{bmatrix} M = M'^T \begin{bmatrix} D' & 0 \\ 0 & D' \end{bmatrix} M'.$$

Putting $N = MM'^{-1}$ we get a symplectic N such that

$$N^T \begin{bmatrix} D & 0 \\ 0 & D \end{bmatrix} N = \begin{bmatrix} D' & 0 \\ 0 & D' \end{bmatrix}.$$

Substituting $N^T = JN^{-1}J^{-1}$ we get

$$N^{-1} \begin{bmatrix} 0 & D \\ -D & 0 \end{bmatrix} N = \begin{bmatrix} 0 & D' \\ -D' & 0 \end{bmatrix}.$$

Identifying the eigenvalues on both sides we get $D = D'$ □

Theorem 2. *A real positive definite matrix* S *is in* K_n *if and only if there exists a diagonal matrix* $D = \mathrm{diag}(d_1, d_2, \ldots, d_n)$ *with* $d_1 \geq d_2 \geq \cdots \geq d_n \geq \frac{1}{2}$ *and a symplectic matrix* $M \in Sp(2n,\mathbb{R})$ *such that*

$$S = M^T \begin{bmatrix} D & 0 \\ 0 & D \end{bmatrix} M. \tag{3.5}$$

In particular,

$$\det S = \prod_i^n d_j^2 \geq 4^{-n}. \tag{3.6}$$

Proof. Let S be a real strictly positive definite matrix in K_n. From (1.3) we have $S \geq \frac{i}{2}J$ and therefore, for any $L \in Sp(2n,\mathbb{R})$,

$$L^T SL \geq \frac{i}{2}J. \tag{3.7}$$

Using Proposition 1 choose L so that

$$L^T SL = \begin{bmatrix} D & 0 \\ 0 & D \end{bmatrix}$$

where $D = \mathrm{diag}(d_1, d_2, \ldots, d_n)$, $d_1 \geq d_2 \geq \cdots \geq d_n > 0$. Now (3.7) implies

$$\begin{bmatrix} D & \frac{i}{2}I \\ -\frac{i}{2}I & D \end{bmatrix} \geq 0.$$

The minor of second order in the left hand side arising from the jj, $jn+j$, $n+jj$, $n+j\,n+j$ entries is $d_j^2 - \frac{1}{4} \geq 0$. Choosing $L = M^{-1}$ we obtain (3.5) and (3.6). Now we drop the assumption of strict positive definiteness on S. From the definition of K_n in (1.3) it follows that for any $S \in K_n$ one has $S + \varepsilon I \in K_n$ for every $\varepsilon > 0$. Since $S+\varepsilon I$ is strictly positive definite $\det S + \varepsilon I \geq 4^{-n}$ $\forall$ $\varepsilon > 0$. Letting $\varepsilon \to 0$ we see that (3.6) holds and S is strictly positive definite.

To prove the converse, consider an arbitrary diagonal matrix $D = \mathrm{diag}(d_1, d_2, \ldots, d_n)$ with $d_1 \geq d_2 \geq \cdots \geq d_n \geq \frac{1}{2}$. Clearly

$$2\begin{bmatrix} D & 0 \\ 0 & D \end{bmatrix} - i\begin{bmatrix} 0 & -I \\ I & 0 \end{bmatrix} \geq 0,$$

and hence for any $M \in Sp(2n,\mathbb{R})$

$$2M^T \begin{bmatrix} D & 0 \\ 0 & D \end{bmatrix} M - i\begin{bmatrix} 0 & -I \\ I & 0 \end{bmatrix} \geq 0.$$

In other words,

$$M^T \begin{bmatrix} D & 0 \\ 0 & D \end{bmatrix} M \in K_n \qquad M \in Sp(2n,\mathbb{R}).$$

Finally, the uniqueness of the parameters $d_1 \geq d_2 \geq \cdots \geq d_n \geq \frac{1}{2}$ in the theorem is a consequence of Proposition 1. $\square$

We now prove an elementary lemma on diagonal matrices before the statement of our next result on the convex set K_n.

Lemma 1. *Let $D \geq I$ be a positive diagonal matrix of order n. Then there exist positive diagonal matrices D_1, D_2 such that*

$$D = \frac{1}{2}(D_1 + D_2) = \frac{1}{2}(D_1^{-1} + D_2^{-1}).$$

Proof. We write $D_2 = D_1 X$ and solve for D_1 and X so that

$$2D = D_1(I + X) = D_1^{-1}(I + X^{-1}),$$

D_1 and X being diagonal. Eliminating D_1 we get the equation

$$(I + X)(I + X^{-1}) = 4D^2$$

which reduces to the quadratic equation

$$X^2 + (2 - 4D^2)X + I = 0.$$

Solving for X we do get a positive diagonal matrix solution

$$X = I + 2(D^2 - 1) + 2D(D^2 - I)^{1/2}.$$

Writing

$$D_1 = 2D(I + X)^{-1}, \quad D_2 = D_1 X$$

we get D_1, D_2 satisfying the required property. $\square$

Theorem 3. *A real positive definite matrix S of order $2n$ belongs to K_n if and only if there exist symplectic matrices L, M such that*

$$S = \frac{1}{4}(L^T L + M^T M).$$

Furthermore, S is an extreme point of K_n if and only if $S = \frac{1}{2} L^T L$ for some symplectic matrix L.

Proof. Let $S \in K_n$. By Theorem 2 we express S as

$$S = N^T \begin{bmatrix} D & 0 \\ 0 & D \end{bmatrix} N \tag{3.8}$$

where N is symplectic and $D = \mathrm{diag}(d_1, d_2, \ldots, d_n)$, $d_1 \geq d_2 \geq \cdots \geq d_n \geq \frac{1}{2}$. Thus $2D \geq I$ and by Lemma 1 there exist diagonal matrices $D_1 > 0$, $D_2 > 0$ such that

$$2D = \frac{1}{2}(D_1 + D_2) = \frac{1}{2}(D_1^{-1} + D_2^{-1}).$$

We rewrite (3.8) as

$$S = \frac{1}{4} N^T \left(\begin{bmatrix} D_1 & 0 \\ 0 & D_1^{-1} \end{bmatrix} + \begin{bmatrix} D_2 & 0 \\ 0 & D_2^{-1} \end{bmatrix} \right) N.$$

Putting

$$L = \begin{bmatrix} D_1^{1/2} & 0 \\ 0 & D_1^{-1/2} \end{bmatrix} N, \quad M = \begin{bmatrix} D_2^{1/2} & 0 \\ 0 & D_2^{-1/2} \end{bmatrix}$$

we have

$$S = \frac{1}{4}(L^T L + M^T M).$$

Since $\begin{bmatrix} D_i^{1/2} & 0 \\ 0 & D_i^{-1/2} \end{bmatrix}$, $i = 1,2$ are symplectic it follows that L and M are symplectic. This proves the only if part of the first half of the theorem.

Since

$$\begin{bmatrix} I & 0 \\ 0 & I \end{bmatrix} - i \begin{bmatrix} 0 & -I \\ I & 0 \end{bmatrix} \geq 0$$

multiplication by L^T on the left and L on the right shows that $L^T L - iJ \geq 0$ for any symplectic L. Hence $\frac{1}{2} L^T L \in K_n \ \forall \ L \in Sp(2n, \mathbb{R})$. Since K_n is convex, $\frac{1}{4}(L^T L + M^T M) \in K_n$, completing the proof of the first part.

The first part also shows that for an element S of K_n to be extremal it is necessary that $S = \frac{1}{2} L^T L$ for some symplectic L. To prove sufficiency, suppose there exist $L \in Sp(2n, \mathbb{R})$, $S_1, S_2 \in K_n$ such that

$$\frac{1}{2} L^T L = \frac{1}{2}(S_1 + S_2).$$

By the first part of the theorem there exist $L_j \in Sp(2n, \mathbb{R})$ such that

$$L^T L = \frac{1}{4} \sum_{j=1}^{4} L_j^T L_j \tag{3.9}$$

where $S_1 = \frac{1}{4}(L_1^T L_1 + L_2^T L_2)$, $S_2 = \frac{1}{4}(L_3^T L_3 + L_4^T L_4)$. Left multiplication by $(L^T)^{-1}$ and right multiplication by L^{-1} on both sides of (3.9) yields

$$I = \frac{1}{4} \sum_{j=1}^{4} M_j \tag{3.10}$$

where

$$M_j = (L^T)^{-1} L_j^T L_j L^{-1}.$$

Each M_j is symplectic and positive definite. Multiplying by J on both sides of (3.10) we get

$$
\begin{aligned}
J &= \frac{1}{4}\sum_{j=1}^{4} M_j J \\
&= \frac{1}{4}\sum_{j=1}^{4} M_j J M_j M_j^{-1} \\
&= \frac{1}{4} J \sum_{j=1}^{4} M_j^{-1}.
\end{aligned}
$$

Thus

$$I = \frac{1}{4}\sum_{j=1}^{4} M_j = \frac{1}{4}\sum_{j=1}^{4} M_j^{-1} = \frac{1}{4}\sum_{j=1}^{4}\frac{1}{2}(M_j + M_j^{-1}),$$

which implies

$$\sum_{j=1}^{4}\left(M_j^{1/2} - M_j^{-1/2}\right)^2 = 0,$$

or

$$M_j = I \quad \forall \quad 1 \leq j \leq 4$$

Thus

$$L_j^T L_j = L^T L \quad \forall \quad j$$

and $S_1 = S_2$. This completes the proof of sufficiency. □

Corollary 1. *Let S_1, S_2 be extreme points of K_n satisfying the inequality $S_1 \geq S_2$. Then $S_1 = S_2$.*

Proof. By Theorem 3 there exist $L_i \in Sp(2n, \mathbb{R})$ such that $S_i = \frac{1}{2} L_i^T L_i$, $i = 1, 2$. Note that $M = L_2 L_1^{-1}$ is symplectic and the fact that $S_1 \geq S_2$ can be expressed as $M^T M \leq I$. Thus the eigenvalues of $M^T M$ lie in the interval $(0, 1]$ but their product is equal to $(\det M)^2 = 1$. This is possible only if all the eigenvalues are unity, i.e., $M^T M = I$. This at once implies $L_1^T L_1 = L_2^T L_2$. □

Using the Williamson's normal form of the covariance matrix and the transformation properties of Gaussian states in Section 3 of [4] we shall now derive a formula for the density operator of a general Gaussian state. As in [4] denote by $\rho_g(\boldsymbol{\ell}, \boldsymbol{m}, S)$ the Gaussian state in $L^2(\mathbb{R}^n)$ with the quantum Fourier transform

$$\rho_g(\boldsymbol{\ell}, \boldsymbol{m}, S)^\wedge(\boldsymbol{z}) = \exp -i\sqrt{2}(\boldsymbol{\ell}^T \boldsymbol{x} - \boldsymbol{m}^T \boldsymbol{y}) - (\boldsymbol{x}^T \boldsymbol{y}^T) S \begin{pmatrix} \boldsymbol{x} \\ \boldsymbol{y} \end{pmatrix}, \boldsymbol{z} = \boldsymbol{x} + i\boldsymbol{y}$$

where $\boldsymbol{\ell}$, $\boldsymbol{m} \in \mathbb{R}^n$ and S has the Williamson's normal form

$$S = M^T \begin{bmatrix} D & 0 \\ 0 & D \end{bmatrix} M$$

with $M \in Sp(2n, \mathbb{R})$, $D = \mathrm{diag}(d_1, d_2, \ldots, d_n)$, $d_1 \geq d_2 \geq \cdots \geq d_n \geq \frac{1}{2}$. From Corollary 3.3 of [4] we have

$$W\left(\frac{\boldsymbol{m}+i\boldsymbol{\ell}}{\sqrt{2}}\right)^{\dagger}\rho_g(\boldsymbol{\ell},\boldsymbol{m},S)W\left(\frac{\boldsymbol{m}+i\boldsymbol{\ell}}{\sqrt{2}}\right)=\rho_g(\mathbf{0},\mathbf{0},S)$$

and Corollary 3.5 of [4] implies

$$\rho_g(\mathbf{0},\mathbf{0},S)=\Gamma(M)^{-1}\rho_g\left(\mathbf{0},\mathbf{0},\begin{bmatrix}D&0\\0&D\end{bmatrix}\right)\Gamma(M).$$

Since $\begin{bmatrix}D&0\\0&D\end{bmatrix}$ is a diagonal covariance matrix

$$\rho_g\left(\mathbf{0},\mathbf{0},\begin{bmatrix}D&0\\0&D\end{bmatrix}\right)=\bigotimes_{j=1}^{n}\rho_g(0.0,d_jI_2)$$

where the j-th component in the right hand side is the Gaussian state in $L^2(\mathbb{R})$ with means 0 and covariance matrix d_jI_2, I_2 denoting the identity matrix of order 2. If $d_j=\frac{1}{2}$ we have

$$\rho_g(0,0,\frac{1}{2}I_2)=|e(0)\rangle\langle e(0)| \text{ in } L^2(\mathbb{R}).$$

If $d_j>1/2$, writing $d_j=\frac{1}{2}\coth\frac{1}{2}s_j$, one has

$$\begin{aligned}\rho_g(0,0,d_jI_2)&=(1-e^{-s_j})e^{-s_ja^{\dagger}a}\\&=2\sinh\frac{1}{2}s_j\;e^{-\frac{1}{2}s_j(p^2+q^2)} \text{ in } L^2(\mathbb{R})\end{aligned}$$

with $a,a^{\dagger},p,q$ denoting the operator of annihilation, creation, momentum and position respectively in $L^2(\mathbb{R})$. We now identify $L^2(\mathbb{R}^n)$ and $L^2(\mathbb{R})^{\otimes n}$ and combine the reductions done above to conclude the following:

Theorem 4. *Let $\rho_g(\boldsymbol{\ell},\boldsymbol{m},S)$ be the Gaussian state in $L^2(\mathbb{R}^n)$ with mean momentum and position vectors $\boldsymbol{\ell},\boldsymbol{m}$ respectively and covariance matrix S with Williamson's normal form*

$$S=M^T\begin{bmatrix}D&0\\0&D\end{bmatrix}M,\quad M\in Sp(2n,\mathbb{R}),$$

$D=\mathrm{diag}(d_1,d_2,\ldots,d_n)$, $d_1\geq d_2\geq\cdots\geq d_m>d_{m+1}=d_{m+2}=\cdots=d_n=\frac{1}{2}$, $d_j=\frac{1}{2}\coth\frac{1}{2}s_j$, $1\leq j\leq m$, $s_j>0$. Then

$$\begin{aligned}\rho_g(\boldsymbol{\ell},\boldsymbol{m},S)=W(\frac{\boldsymbol{m}+i\boldsymbol{\ell}}{\sqrt{2}})\Gamma(M)^{-1}\prod_{j=1}^{m}(1-e^{-s_j})\times\\ e^{-\Sigma_{j=1}^{m}s_ja_j^{\dagger}a_j}\otimes(|e(0)\rangle\times\langle e(0)|)^{\otimes n-m}\Gamma(M)W(\frac{\boldsymbol{m}+i\boldsymbol{\ell}}{\sqrt{2}})^{-1}\end{aligned}\quad(3.11)$$

where $W(\cdot)$ denotes Weyl operator, $\Gamma(M)$ is the unitary operator implementing the Bogolioubov automorphism of CCR corresponding to the symplectic linear trans-

formation M and $|e(0)\rangle$ denotes the exponential vector corresponding to 0 *in any copy of* $L^2(\mathbb{R})$.

Proof. Immediate from the discussion preceding the statement of the theorem. □

Corollary 2. *The wave function of the most general pure Gaussian state in*$L^2(\mathbb{R}^n)$ *is of the form*

$$|\psi\rangle = W(\boldsymbol{\alpha})\Gamma(U)\,|e_{\lambda_1}\rangle|e_{\lambda_2}\rangle\cdots|e_{\lambda_n}\rangle$$

where

$$e_\lambda(x) = (2\pi)^{-1/4}\lambda^{-1/2}\exp -4^{-1}\lambda^{-2}x^2, \quad x\in\mathbb{R}, \lambda > 0,$$

$\boldsymbol{\alpha}\in\mathbb{C}^n$, *$U$ is a unitary matrix of order n, $W(\boldsymbol{\alpha})$ is the Weyl operator associated with $\boldsymbol{\alpha}$, $\Gamma(U)$ is the second quantization unitary operator associated with U and λ_j, $1\le j\le n$ are positive scalars.*

Proof. Since the number operator $a^\dagger a$ has spectrum $\{0,1,2,\dots\}$ it follows from Theorem 4 that $\rho_g(\boldsymbol{\ell},\boldsymbol{m},S)$ is pure if and only if $m=0$ in (3.11). This implies that the corresponding wave function $|\psi\rangle$ can be expressed as

$$|\psi\rangle = W(\boldsymbol{\alpha})\Gamma(M)^{-1}(|e(0)\rangle)^{\otimes n} \tag{3.12}$$

where $M\in Sp(2n,\mathbb{R})$ and $\boldsymbol{\alpha} = \frac{\boldsymbol{m}+i\boldsymbol{\ell}}{\sqrt{2}}$. The covariance matrix of this pure Gaussian state is $\frac{1}{2}M^TM$. The symplectic matrix M has the decomposition [1]

$$M = V_1\begin{bmatrix} D & 0 \\ 0 & D^{-1}\end{bmatrix}V_2$$

where V_1 and V_2 are real orthogonal as well as symplectic and D is a positive diagonal matrix of order n. Thus

$$\begin{aligned} M^TM &= V_2^T\begin{bmatrix} D^2 & 0 \\ 0 & D^{-2}\end{bmatrix}V_2 \\ &= N^TN \end{aligned}$$

where

$$N = \begin{bmatrix} D & 0 \\ 0 & D^{-1}\end{bmatrix}V_2.$$

Since the covariance matrix of $|\psi\rangle$ in (3.12) can also be written as $\frac{1}{2}N^TN$, modulo a scalar multiple of modulus unity $|\psi\rangle$ can also be expressed as

$$|\psi\rangle = W(\boldsymbol{\alpha})\Gamma(V_2)^{-1}\Gamma\left(\begin{bmatrix} D^{-1} & 0 \\ 0 & D\end{bmatrix}\right)\,|e(0)\rangle^{\otimes n}. \tag{3.13}$$

If U is the complex unitary matrix of order n satisfying

$$\begin{aligned} U(\boldsymbol{x}+i\boldsymbol{y}) &= \boldsymbol{x}'+i\boldsymbol{y}', \\ \begin{bmatrix}\boldsymbol{x}'\\ \boldsymbol{y}'\end{bmatrix} &= V_2^T\begin{bmatrix}\boldsymbol{x}\\ \boldsymbol{y}\end{bmatrix} \quad \forall \quad \boldsymbol{x},\boldsymbol{y}\in\mathbb{R}^n \end{aligned}$$

and $D^{-1}=\operatorname{diag}(\lambda_1,\lambda_2,\dots,\lambda_n)$ we can express (3.13) as

$$\begin{aligned} |\psi\rangle &= W(\boldsymbol{\alpha})\Gamma(U)\left\{\bigotimes_{j=1}^{n} \Gamma\left(\begin{bmatrix}\lambda_j & 0\\ 0 & \lambda_j^{-1}\end{bmatrix}\right)|e(0)\rangle\right\} \\ &= W(\boldsymbol{\alpha})\Gamma(U)\,|e_{\lambda_1}\rangle|e_{\lambda_2}\rangle\cdots|e_{\lambda_n}\rangle \end{aligned}$$

where we have identified $L^2(\mathbb{R}^n)$ with $L^2(\mathbb{R})^{\otimes n}$.

We conclude this section with a result on the purification of Gaussian states. □

Theorem 5. *Let ρ be a mixed Gaussian state in $L^2(\mathbb{R}^n)$. Then there exists a pure Gaussian state $|\psi\rangle$ in $L^2(\mathbb{R}^n)\otimes L^2(\mathbb{R}^n)$ such that*

$$\rho = \operatorname{Tr}_2 U\,|\psi\rangle\langle\psi|U^\dagger$$

for some unitary operator U in $L^2(\mathbb{R}^n)\otimes L^2(\mathbb{R}^n)$ with Tr_2 *denoting the relative trace over the second copy of $L^2(\mathbb{R}^n)$.*

Proof. First we remark that by a Gaussian state in $L^2(\mathbb{R}^n)\otimes L^2(\mathbb{R}^n)$ we mean it by the canonical identification of this product Hilbert space with $L^2(\mathbb{R}^{2n})$. Let $\rho=\rho_g(\boldsymbol{\ell},\boldsymbol{m},S)$ where by Theorem 3 we can express

$$S=\frac{1}{4}\left(L_1^TL_1+L_2^TL_2\right),\quad L_1,L_2\in Sp(2n,\mathbb{R}).$$

Now consider the pure Gaussian states,

$$|\psi_{L_i}\rangle=\Gamma(L_i)^{-1}\,|e(\mathbf{0})\rangle,\quad i=1,2$$

in $L^2(\mathbb{R}^n)$ and the second quantization unitary operator Γ_0 satisfying

$$\Gamma_0\, e(\boldsymbol{u}\oplus\boldsymbol{v})=e\left(\frac{\boldsymbol{u}+\boldsymbol{v}}{\sqrt{2}}\oplus\frac{\boldsymbol{u}-\boldsymbol{v}}{\sqrt{2}}\right)\quad \forall\,\boldsymbol{u},\boldsymbol{v}\in\mathbb{C}^n$$

in $L^2(\mathbb{R}^{2n})$ identified with $L^2(\mathbb{R}^n)\otimes L^2(\mathbb{R}^n)$, so that

$$e(\boldsymbol{u}\oplus\boldsymbol{v})=e(\boldsymbol{u})\otimes e(\boldsymbol{v}).$$

Then by Proposition 3.11 of [4] we have

$$\operatorname{Tr}_2\,\Gamma_0\left(|\psi_{L_1}\rangle\langle\psi_{L_1}|\otimes|\psi_{L_2}\rangle\langle\psi_{L_2}|\right)\Gamma_0^\dagger=\rho_g(\mathbf{0},\mathbf{0},S).$$

If $\boldsymbol{\alpha}=\frac{\boldsymbol{m}+i\boldsymbol{\ell}}{\sqrt{2}}$ we have

$$W(\boldsymbol{\alpha})\rho_g(\mathbf{0},\mathbf{0},S)W(\boldsymbol{\alpha})^\dagger = \rho_g(\boldsymbol{\ell},\boldsymbol{m},S).$$

Putting

$$U = (W(\boldsymbol{\alpha})\otimes I)\Gamma_0\left(\Gamma(L_1)^{-1}\otimes\Gamma(L_2)^{-1}\right)$$

we get

$$\rho_g(\boldsymbol{\ell},\boldsymbol{m},S) = \mathrm{Tr}_2\, U\, |e(\mathbf{0})\otimes e(\mathbf{0})\rangle\langle e(\mathbf{0})\otimes e(\mathbf{0})|\, U^\dagger$$

where $|e(\mathbf{0})\rangle$ is the exponential vector in $L^2(\mathbb{R}^n)$. □

4 The symmetry group of the set of Gaussian states

Let S_n denote the set of all Gaussian states in $L^2(\mathbb{R})$. We say that a unitary operator U in $L^2(\mathbb{R}^n)$ is a *Gaussian symmetry* if, for any $\rho\in S_n$, the state $U\rho U^\dagger$ is also in S_n. All such Gaussian symmetries constitute a group $\mathscr{G}_n$. If $\boldsymbol{\alpha}\in\mathbb{C}^n$ and $L\in Sp(2n,\mathbb{R})$ then the associated Weyl operator $W(\boldsymbol{\alpha})$ and the unitary operator $\Gamma(L)$ implementing the Bogolioubov automorphism of CCR corresponding to L are in $\mathscr{G}_n$ (See Corollary 3.5 in [4].) The aim of this section is to show that any element U in $\mathscr{G}_n$ is of the form $\lambda W(\boldsymbol{\alpha})\Gamma(L)$ where λ is a complex scalar of modulus unity, $\boldsymbol{\alpha}\in\mathbb{C}^n$ and $L\in Sp(2n,\mathbb{R})$. This settles a question raised in [4].

We begin with a result on a special Gaussian state.

Theorem 6. *Let $s_1 > s_2 > \cdots > s_n > 0$ be irrational numbers which are linearly independent over the field Q of rationals and let*

$$\rho_{\mathbf{s}} = \rho_g(\mathbf{0},\mathbf{0},S) = \prod_{j=1}^n (1-e^{-s_j})e^{-\sum_{j=1}^n s_j a_j^\dagger a_j}$$

be the Gaussian state in $L^2(\mathbb{R}^n)$ with zero position and momentum mean vectors and covariance matrix

$$S = \begin{bmatrix} D & 0\\ 0 & D\end{bmatrix},\quad D = \mathrm{diag}(d_1,d_2,\ldots,d_n)$$

with $d_j = \frac{1}{2}\coth\frac{1}{2}s_j$. Then a unitary operator U in $L^2(\mathbb{R}^n)$ has the property that $U\rho_{\mathbf{s}}U^\dagger$ is a Gaussian state if and only if, for some $\boldsymbol{\alpha}\in\mathbb{C}^n$, $L\in Sp(2n,\mathbb{R})$ and a complex-valued function β of modulus unity on $\mathbb{Z}_+^n$

$$U = W(\boldsymbol{\alpha})\Gamma(L)\beta(a_1^\dagger a_1, a_2^\dagger a_2,\ldots,a_n^\dagger a_n) \tag{4.1}$$

where $\mathbb{Z}_+ = \{0,1,2,\ldots\}$.

Proof. Sufficiency is immediate from Corollary 3.3 and Corollary 3.5 of [4]. To prove necessity assume that

$$U\rho_{\mathbf{s}}U^\dagger = \rho_g(\boldsymbol{\ell},\boldsymbol{m},S') \tag{4.2}$$

Since $a^\dagger a$ in $L^2(\mathbb{R})$ has spectrum $\mathbb{Z}_+$ and each eigenvalue k has multiplicity one [2] it follows that the selfadjoint positive operator $\sum_{j=1}^n s_j a_j^\dagger a_j$, being a sum of commuting self adjoint operators $s_j a_j^\dagger a_j$, $1 \leq j \leq n$ has spectrum $\left\{ \sum_{j=1}^n s_j k_j \middle| k_j \in \mathbb{Z}_+ \ \forall\ j \right\}$ with each eigenvalue of multiplicity one thanks to the assumption on $\{s_j, 1 \leq j \leq n\}$. Since $\rho_{\boldsymbol{s}}$ and $U\rho_{\boldsymbol{s}}U^{-1}$ have the same set of eigenvalues and same multiplicities it follows from Theorem 4 that

$$U\rho_{\boldsymbol{s}}U^{-1} = W(\boldsymbol{z})\Gamma(M)^{-1}\rho_{\boldsymbol{t}}\Gamma(M)W(\boldsymbol{z})^{-1} \tag{4.3}$$

where $\boldsymbol{z} \in \mathbb{C}^n$, $M \in Sp(2n,\mathbb{R})$, $\boldsymbol{t} = (t_1, t_2, \dots, t_n)^T$ and

$$\rho_{\boldsymbol{t}} = \prod_{j=1}^n (1 - e^{-t_j}) e^{-\sum_{j=1}^n t_j a_j^\dagger a_j}.$$

Since the maximum eigenvalues of $\rho_{\boldsymbol{s}}$ and $\rho_{\boldsymbol{t}}$ are same it follows that

$$\prod (1 - e^{-s_j}) = \prod (1 - e^{-t_j}).$$

Since the spectra of $\rho_{\boldsymbol{s}}$ and $\rho_{\boldsymbol{t}}$ are same it follows that

$$\left\{ \sum_{j=1}^n s_j k_j \middle| k_j \in \mathbb{Z}_+ \quad \forall\ j \right\} = \left\{ \sum_{j=1}^n t_j k_j \middle| k_j \in \mathbb{Z}_+ \quad \forall\ j \right\}.$$

Choosing $\boldsymbol{k} = (0, 0, \dots, 0, 1, 0, \dots, 0)^T$ with 1 in the k-th position we conclude the existence of matrices A, B of order $n \times n$ and entries in $\mathbb{Z}_+$ such that

$$\boldsymbol{t} = A\boldsymbol{s}, \quad \boldsymbol{s} = B\boldsymbol{t}$$

so that $BA\boldsymbol{s} = \boldsymbol{s}$. The rationally linear independence of the s_j's implies $BA = I$. This is possible only if A and $B = A^{-1}$ are both permutation matrices.

Putting $V = \Gamma(M)W(\boldsymbol{z})^\dagger U$ we have from (4.3)

$$V\rho_{\boldsymbol{s}} = \rho_{\boldsymbol{t}} V.$$

Denote by $|\boldsymbol{k}\rangle$ the vector satisfying

$$a_j^\dagger a_j\ |\boldsymbol{k}\rangle = k_j\ |\boldsymbol{k}\rangle$$

where $|\boldsymbol{k}\rangle = |k_1\rangle |k_2\rangle \cdots |k_n\rangle$. Then

$$\begin{aligned} V\rho_{\boldsymbol{s}}\ |\boldsymbol{k}\rangle &= \prod_{j=1}^n (1 - e^{-s_j}) e^{-\sum s_j k_j}\ V\ |\boldsymbol{k}\rangle \\ &= \rho_{\boldsymbol{t}} V |\boldsymbol{k}\rangle, \quad \boldsymbol{k} \in \mathbb{Z}_+^n. \end{aligned}$$

Thus $V|\boldsymbol{k}\rangle$ is an eigenvector for $\rho_{\boldsymbol{t}}$ corresponding to the eigenvalue

$$\begin{aligned}\prod(1-e^{-s_j})e^{-\boldsymbol{s^t k}} &= \prod_{j=1}^{n}(1-e^{-t_j})e^{-\boldsymbol{t}^T B^T \boldsymbol{k}} \\ &= \prod_{j=1}^{n}(1-e^{-t_j})e^{-\boldsymbol{t}^T A\boldsymbol{k}}.\end{aligned}$$

Hence there exists a scalar $\beta(\boldsymbol{k})$ of modulus unity such that

$$\begin{aligned}V\,|\boldsymbol{k}\rangle &= \beta(\boldsymbol{k})\,|A\boldsymbol{k}\rangle \\ &= \Gamma(A)\beta(a_1^\dagger a_1, a_2^\dagger a_2, \ldots, a_n^\dagger a_n)\,||\boldsymbol{k}\rangle\ \forall\ \boldsymbol{k}\in\mathbb{Z}_+^n.\end{aligned}$$

where $\Gamma(A)$ is the second quantization of the permutation unitary matrix A acting in $\mathbb{C}^n$. Thus

$$U = W(\boldsymbol{z})\Gamma(M)^\dagger\Gamma(A)\beta(a_1^\dagger a_1, a_2^\dagger a_2, \ldots, a_n^\dagger a_n).$$

which completes the proof. $\square$

Theorem 7. *A unitary operator U in $L^2(\mathbb{R}^n)$ is a Gaussian symmetry if and only if there exist a scalar λ of modulus unity, a vector $\boldsymbol{\alpha}$ in $\mathbb{C}^n$ and a symplectic matrix $L\in Sp(2n,\mathbb{R})$ such that*

$$U = \lambda W(\boldsymbol{\alpha})\Gamma(L)$$

where $W(\boldsymbol{\alpha})$ is the Weyl operator associated with $\boldsymbol{\alpha}$ and $\Gamma(L)$ is a unitary operator implementing the Bogolioubov automorphism of CCR corresponding to L.

Proof. The if part is already contained in Corollary 3.3 and Corollary 3.5 of [4]. In order to prove the only if part we may, in view of Theorem 6, assume that $U = \beta(a_1^\dagger a_1, a_2^\dagger a_2, \ldots, a_n^\dagger a_n)$ where β is a function of modulus unity on $\mathbb{Z}_+^n$. If such a U is a Gaussian symmetry then, for any pure Gaussian state $|\psi\rangle$, $U|\psi\rangle$ is also a pure Gaussian state. We choose

$$|\psi\rangle = e^{-\frac{1}{2}\|\boldsymbol{u}\|^2}|e(\boldsymbol{u})\rangle = W(\boldsymbol{u})|e(\boldsymbol{0})\rangle$$

where $\boldsymbol{u} = (u_1, u_2, \ldots, u_n)^T \in \mathbb{C}^n$ with $u_j \neq 0\ \forall\ j$. By our assumption

$$|\psi'\rangle = e^{-\frac{1}{2}\|\boldsymbol{u}\|^2}\beta(a_1^\dagger a_1, a_2^\dagger a_2, \ldots, a_n^\dagger a_n)|e(\boldsymbol{u})\rangle \tag{4.4}$$

is also a pure Gaussian state. By Corollary 2, $\exists\boldsymbol{\alpha}\in\mathbb{C}^n$, a unitary matrix A of order n and $\lambda_j > 0$, $1\le j\le n$ such that

$$|\psi'\rangle = W(\boldsymbol{\alpha})\Gamma(A)\,|e_{\lambda_1}\rangle|e_{\lambda_2}\rangle\cdots|e_{\lambda_n}\rangle. \tag{4.5}$$

Using (4.4) and (4.5) we shall evaluate the function $f(\boldsymbol{z}) = \langle\psi'|e(\boldsymbol{z})\rangle$ in two different ways. From (4.4) we have

$$\begin{aligned} f(\boldsymbol{z}) &= e^{-\frac{1}{2}\|\boldsymbol{u}\|^2} \langle e(\boldsymbol{u}) \left| \overline{\beta}(a_1^\dagger a_1, a_2^\dagger a_2, \dots, a_n^\dagger a_n) \right| e(\boldsymbol{z}) \rangle \\ &= e^{-\frac{1}{2}\|\boldsymbol{u}\|^2} \sum_{\boldsymbol{z}\in\mathbb{Z}_+^n} \frac{\overline{\beta}(k_1,k_2,\dots,k_n)}{k_1!k_2!\dots k_n!} (\overline{u}_1 z_1)^{k_1} \dots (\overline{u}_n z_n)^{k_n} \, |k_1 k_2 \cdots k_n\rangle \end{aligned} \tag{4.6}$$

where $|k_1 k_2 \cdots k_n\rangle = |k_1\rangle |k_2\rangle \cdots |k_n\rangle$ and $|e(z)\rangle = \sum_{k\in\mathbb{Z}_+} \frac{z^k}{\sqrt{k!}} |k\rangle$ for $z \in \mathbb{C}$.

Since $|\beta(\boldsymbol{k})| = 1$, (4.6) implies

$$|f(\boldsymbol{z})| \le \exp\left\{ -\frac{1}{2}\|\boldsymbol{u}\|^2 + \sum_{j=1}^n |u_j| \, |z_j| \right\}. \tag{4.7}$$

From the definition of $|e_\lambda\rangle$ in Corollary 2 and the exponential vector $|e(z)\rangle$ in $L^2(\mathbb{R})$ one has

$$\langle e_\lambda | e(z)\rangle = \sqrt{\frac{2\lambda}{1+\lambda^2}} \exp \frac{1}{2} \left(\frac{\lambda^2 - 1}{\lambda^2 + 1} \right) z^2, \quad \lambda > 0, \quad z \in \mathbb{C}.$$

This together with (4.5) implies

$$\begin{aligned} f(\boldsymbol{z}) &= \langle e_{\lambda_1} \otimes e_{\lambda_2} \otimes \cdots \otimes e_{\lambda_n} \left| \Gamma(A^{-1}) W(-\boldsymbol{\alpha}) e(\boldsymbol{z}) \right\rangle \\ &= e^{\langle \boldsymbol{\alpha} | \boldsymbol{z}\rangle - \frac{1}{2}\|\boldsymbol{\alpha}\|^2} \langle e_{\lambda_1} \otimes e_{\lambda_2} \otimes \cdots \otimes e_{\lambda_n} \left| e(A^{-1}(\boldsymbol{z} + \boldsymbol{\alpha})) \right\rangle \end{aligned}$$

which is a nonzero scalar multiple of the exponential of a polynomial of degree 2 in $z_1, z_2, \dots, z_n$ except when all the λ_j's are equal to unity. This would contradict the inequality (4.6) except when $\lambda_j = 1 \; \forall \; j$. Thus $\lambda_j = 1 \; \forall \; j$ and (4.5) reduces to

$$\begin{aligned} |\psi'\rangle &= W(\boldsymbol{\alpha}) \Gamma(A) \, |e(\boldsymbol{0}\rangle \\ &= e^{-\frac{1}{2}\|\boldsymbol{\alpha}\|^2} \, |e(\boldsymbol{\alpha})\rangle. \end{aligned}$$

Now (4.4) implies

$$\begin{aligned} &\beta(a_1^\dagger a_1, a_2^\dagger a_2, \dots, a_n^\dagger a_n) \, |e(\boldsymbol{u})\rangle \\ &= e^{\frac{1}{2}(\|\boldsymbol{u}\|^2 - \|\boldsymbol{\alpha}\|^2)} \, |e(\boldsymbol{\alpha})\rangle, \end{aligned}$$

or

$$\begin{aligned} &\sum_{\boldsymbol{k}\in\mathbb{Z}_+^n} \frac{u_1^{k_1} u_2^{k_2} \dots u_n^{k_n}}{\sqrt{k_1!} \cdots \sqrt{k_n!}} \beta(k_1, k_2, \dots, k_n) \, |k_1 k_2 \dots k_n\rangle \\ &= e^{\frac{1}{2}(\|\boldsymbol{u}\|^2 - \|\boldsymbol{\alpha}\|^2)} \sum \frac{\alpha_1^{k_1} \alpha_2^{k_2} \dots \alpha_n^{k_n}}{\sqrt{k_1!} \cdots \sqrt{k_n!}} \, |k_1 k_2 \dots k_n\rangle. \end{aligned}$$

Thus

$$\beta(k_1, k_2, \ldots, k_n) = e^{\frac{1}{2}(\|\boldsymbol{u}\|^2 - \|\boldsymbol{\alpha}\|^2)} \left(\frac{\alpha_1}{u_1}\right)^{k_1} \cdots \left(\frac{\alpha_n}{u_n}\right)^{k_n}.$$

Since $|\beta(\boldsymbol{k})| = 1$ and $u_j \neq 0 \,\forall\, j$ it follows that $|\frac{\alpha_j}{u_j}| = 1$ and

$$\beta(\boldsymbol{k}) = e^{i \sum_{j=1}^{n} \theta_j k_j} \quad \forall\, \boldsymbol{k} \in \mathbb{Z}_+^n$$

where θ_j's are real. Thus $\beta(a_1^\dagger a_1, a_2^\dagger a_2, \ldots, a_n^\dagger a_n) = \Gamma(D)$, the second quantization of the diagonal unitary matrix $D = \operatorname{diag}(e^{i\theta_1}, e^{i\theta_2}, \ldots, e^{i\theta_n})$. This completes the proof. $\square$

References

1. Arvind, Dutta, B., Mukunda, N. and Simon, R. : The real symplectic groups in quantum mechanics and optics, Pramana – Journal of Physics **45** (1995) 471-497.

2. Gardiner, C. W. : Quantum Noise, Springer-Verlag, Berlin, 1992.

3. Holevo, A. S. : Probablistic and Statistical Aspects of Quantum Theory, North Holland, Amsterdam, 1982.

4. Parthasarathy, K. R. : What is a Gaussian state? Communications on Stochastic Analysis **4** (2010) 143-160.

5. Parthasarathy, K. R. : An Introduction to Quantum Stochastic Calculus, Birkhaüser, Basel, 1992.